



WIRELESS STIG

APRIVA SENSa SECURE MOBILE E-MAIL SYSTEM SECURITY CHECKLIST

Version 5, Release 2.2

14 April 2009

Developed by DISA for the DoD

Database Reference Number: _____

CAT I: _____

Database entered by: _____ Date: _____

CAT II: _____

Technical Q/A by: _____ Date: _____

CAT III: _____

Final Q/A by: _____ Date: _____

CAT IV: _____

TOTAL: _____

UNCLASSIFIED

Unclassified UNTIL FILLED IN

CIRCLE ONE

FOR OFFICIAL USE ONLY (mark each page)

CONFIDENTIAL and SECRET (mark each page and each finding)

Classification is based on classification of system reviewed:

Unclassified System = FOUO Checklist

Confidential System = CONFIDENTIAL Checklist

Secret System = SECRET Checklist

Top Secret System = SECRET Checklist

Site Name: _____ **Date of Wireless**

SRR: _____

Wireless Reviewer		Phone/Location		
Previous SRR (circle)	Y N	Date of Previous SRR		
Number of Current Open Findings				
Site Name				
Address				
Phone				
Position	Name	Phone Number	Email	Area of Responsibility
IAM				
IAO				
Sensa Administrator				

This page is intentionally blank.

TABLE OF CONTENTS

	Page
SUMMARY OF CHANGES.....	IX
1. INTRODUCTION.....	1
2. APRIVA SENSА COMPLIANCE REQUIREMENTS	3
2.1 Classified Information	3
WIR0180 Wireless PEDs allowed into Sensitive Compartmented Information Facilities (SCIFs) must be Director Central Intelligence Directive (DCID) compliant. .	3
WIR0225 Use proper separation when using Wireless PEDs around classified areas. .	4
WIR0372 Do not allow PEDs with cameras into classified processing areas.	5
WIR1010 Establish CMI procedures for Wireless PEDs and systems.	6
WIR1020 Do not use wireless e-mail for classified messages.	6
WIR1040 Do not connect wireless e-mail to classified computers.	7
2.2 Unclassified Information	8
WIR0010 All wireless systems must have DAA approval.	8
WIR0011 Personally owned PEDs need DAA approval and forfeiture agreement.	9
WIR0012 Display required DoD logon banner on PDA.	9
WIR0016 Maintain an equipment list of all approved wireless devices.	11
WIR0030 Document equipment in the SSP.....	11
WIR0072 Wireless network devices must be physically protected.....	12
WIR0076 Require signed user agreement.	12
WIR0371 PEDs with cameras must be approved by physical security policies.....	15
WIR1015 Establish disposal procedures for Sensa Wireless PEDs and systems.	16
WIR1080 Install Wireless e-mail servers using an approved architecture.	17
WIR1090 Required actions if Wireless e-mail handheld is lost or stolen.	18
WIR1100 Authenticated login procedures to unlock a wireless e-mail device.	19
WIR1120 Wireless e-mail handhelds are set to lock after no more than 15 minutes of inactivity.	19
WIR1140 Bluetooth usage must be compliant.	20
WIR1150 Bluetooth Smart Card Reader usage must be compliant.....	20
WIR1160 Secure wireless e-mail servers using operating system STIG.	21
WIR1170 Comply with provisioning requirements for new/re-issued wireless e-mail devices.....	21
WIR1180 Do not allow users to install or remove applications.	22
WIR1200 Digitally sign emergency and/or critical e-mail notifications.....	22
WIR1210 Configure wireless email auto signature as required.	23
WIR1220 If Text Messaging is used, enable security.	23
WIR1280 Data-at-rest encryption is enabled on all wireless e-mail devices.	25
3. SENSА SECURITY RELATED CONFIGURATIONS.....	26
3.1 Known System Limitations.....	26
3.2 Sensa System Architecture	26
3.3 Sensa System Setup and Provisioning	29

3.3.1	Sensa Server Installation.....	29
3.3.2	Windows Mobile Handheld Provisioning.....	30
3.4	Setting Up Certificate Store Password.....	30
3.5	Setting Up Certificate Store and Service and Administrative Accounts	30
3.5.1	Sensa Service Accounts	30
3.5.2	Sensa Admin Accounts	30
3.5.3	Trust Digital Accounts.....	31
3.6	OCSP Configuration	31
3.7	Setting up Security Policies	32
3.7.1	Admin Accounts	32
3.7.2	User Accounts.....	32
3.8	Control of Device Applications	33
3.9	Bluetooth Security Settings.....	33
3.10	Bluetooth Smart Card Reader	33
3.11	Enclave Firewall Configuration Requirements.....	33
APPENDIX A. REFERENCES		35
APPENDIX B. SECURITY POLICY RULES.....		37
APPENDEX C. ALLOCATION OF SECURITY REQUIREMENTS TO APRIVA SENS SYSTEM COMPONENTS		45
APPENDIX D. CAC DIGITAL CERTIFICATE PROVISIONING		55
APPENDIX E. VMS PROCEDURES.....		57

TABLE OF TABLES

	Page
Table B-1. Sensa Security Policy Rules	37
Table B-2. Trust Digital Security Policy Rule.....	41
Table B-3. Symantec Antivirus Configuration Setting.....	42
Table B-4. Windows Mobile 5.0 with Sensa & Trust Digital Configuration Settings	43
Table C-1. Allocation of DoD Security Requirements to System Components.....	54
Table E-1. VMS Asset Matrix	58

TABLE OF FIGURES

Figure 3-1. Apriva Sensa System Architecture without ISA Server	29
Figure 3-2. OCSP Setup Screen.....	32

This page is intentionally blank.

SUMMARY OF CHANGES

- The previous version of the document was V5R2.1, 5 Nov 2007.

SECTION 2.

- WIR0076: Updated requirement based on DoD CIO Memorandum “Policy on Use of Department of Defense (DoD) Information Systems Standard Consent Banner and User Agreement,” dated 9 May 2008.

SECTION 3.

- WIR0012: Updated check.

This page is intentionally blank.

1. INTRODUCTION

The *Wireless STIG Apriva Sensa Secure Mobile E-mail System Checklist* provides required installation, configuration, and operating instructions of Sensa secure mobile e-mail in the Department of Defense (DoD). Guidance in this document applies to all Sensa systems, including Windows Mobile PDAs and smartphones with the Sensa client installed, and both the Sensa Management Server and Sensa Mail Server (except as noted in the following paragraph).

This document does not apply to Sensa installations supporting Secure Mobile Environment – Portable Electronic Device (SME-PED) systems. Please refer to the *Wireless STIG SME-PED Security Checklist* for security configuration guidance for Sensa installations supporting those systems.

This checklist serves as both a security review checklist and a configuration guide. Information Assurance Officers (IAOs), Security Managers (SMs), System Administrators (SAs), device users, and security readiness reviewers, each with varying experience levels, will use this document to ensure the security of Sensa implementations. Thus, the format of each section is tailored to meet these various needs.

Section 2 should be used by IAOs, SMs, and SAs when performing self-assessments. This section is also used by DISA FSO to perform Security Readiness Reviews (SRRs). Appendix E provides procedures used by SAs and SRR reviewers when registering and updating assets in the Vulnerability Management System (VMS).

Section 3 and Appendices B, C, and D are intended primarily for Sensa SAs and provide security-related requirements for system installation, setup, and configuration. The configuration settings (or actions) in Appendix B are classified as either “Required” or “Optional”. “Required” configuration settings are mandatory for all installations of Sensa in DoD. “Optional” settings are the recommended and preferred configurations for Sensa. “Optional” configuration settings may not be possible at all DoD installations because of operational or network constraints.

This checklist covers configuration requirements for Sensa version 1.9.2, Trust Digital 7.3, and Windows Mobile 5.0. (Sensa currently supports WM 6.0 and Trust Digital is expected to support WM 6.0 in the near future.) Earlier versions of these products should not be used because some required security features are not available.

This document provides the minimum “baseline” Sensa security guidance for DoD. Combatant Commanders/Services/Agencies (CC/S/A) may direct more secure configuration settings based on operational requirements.

For our North Atlantic Treaty Organization (NATO) customers using this document:

The term “classified” used in this document refers to U.S. Government classifications of Confidential, Secret and Top Secret. NATO Sensa deployments are permitted to carry information bearing a NATO classification of “NATO restricted” and should be treated in a similar manner as U.S. Government information marked Unclassified//For Official Use Only.

The security guidance provided in this document can be directly applied to NATO Sensa deployments with the understanding that “NATO Restricted” information should not be equated to US Government-defined “classified” information.

Acknowledgment

DISA FSO would like to acknowledge the support of the Army Advanced Technologies office, Program Executive Office Enterprise Information Systems, located in Fort Belvoir, Virginia in the development of this document.

2. APRIVA SENSa COMPLIANCE REQUIREMENTS

2.1 Classified Information

WIR0180 Wireless PEDs allowed into Sensitive Compartmented Information Facilities (SCIFs) must be Director Central Intelligence Directive (DCID) compliant.

CAT I	WIR0180	V0012072	MAC: 1, 2, 3	CL: C, S	IAC: ECWN-1	Ref: DCID 6/9 and 6/3
Vulnerability: PEDs are allowed in a SCIF without DCID compliance						
The IAO will ensure wireless PEDs (e.g., wireless two-way e-mail devices such as the BlackBerry) are not permitted in a SCIF unless approved in accordance with DCID 6/9 or 6/3 requirements.						
Check: Work with the traditional security reviewer or interview the IAO or SM to verify the following: 1. Determine if site SCIF security policy/procedures allow users to bring PEDs into SCIFs. 2. If No, determine if procedures are in place to prevent users from bringing PEDs into SCIFs and users are trained on this requirement. Posted signs are also evidence of compliance. 3. If Yes, – Determine if site has written procedures that describe what type of PEDs and under what type of conditions (e.g., turned off, SCIF mode enabled). – If PED devices are allowed, then users should receive proper training on the handling of these devices in a SCIF. 4. Mark this as a finding if: – Required procedures or training policies are not in place or – Required user training has not been documented.						
Comments:						
Open		Not a Finding		Not Reviewed		Not Applicable

WIR0225 Use proper separation when using Wireless PEDs around classified areas.

CAT II	WIR0225	V0012106	MAC: 1, 2, 3	CL: C	IAC: ECWN-1	Ref: DoDD 8100.2
Vulnerability: Wireless PEDs are used in classified areas.						
<p>The IAO will ensure wireless PEDs are not permitted or used in areas where classified data processing takes place unless:</p> <ul style="list-style-type: none">– The Designated Approving Authority (DAA), in consultation with the CTTA, has approved the wireless PED for entry and/or use in the facility.– The wireless PED is separated from the classified data equipment a distance determined by the CTTA and appropriate countermeasures, as determined by the CTTA, are implemented.						
Check: Review documentation. Work with the traditional security reviewer to verify the following: <ol style="list-style-type: none">1. If classified information is not processed at this site or site has a written procedure prohibiting the use of wireless devices in areas where classified data processing occurs, then mark as not a finding.2. Ask for documentation showing the CTTA was consulted about operation and placement of wireless devices. Acceptable proof would be coordination signature or initials of the CTTA on the architecture diagram or other evidence of coordination. In accordance with (IAW) DoD policy, the CTTA must have a written separation policy for each classified area.3. Review written policies, training material, or user agreements to see if wireless usage in these areas is addressed.4. Verify proper procedures for wireless device use in classified areas is addressed in training program.5. Mark as a finding if any of the following is found:<ul style="list-style-type: none">– CTTA has not designated a separation distance in writing.– DAA has not coordinated with the CTTA.– Users are not trained or made aware (using signage or user agreement) of procedures wireless device usage in and around classified processing areas.						
Comments:						
Open	<input type="checkbox"/>	Not a Finding	<input type="checkbox"/>	Not Reviewed	<input type="checkbox"/>	Not Applicable

WIR0372 Do not allow PEDs with cameras into classified processing areas.

CAT I	WIR0372	V0012165	MAC: 1, 2, 3	CL: S, P	IAC: DCHW-1	Ref: DoDD 8100.2
Vulnerability: Wireless phones with cameras are allowed into classified areas.						
<p>The IAO will ensure PEDs with digital cameras (still or video) are not allowed in any SCIF or other area where classified documents or information is stored, transmitted, or processed.</p> <p>Check: Interview the IAO and confirm compliance by reviewing site's physical security policy. The traditional security reviewer may also assist in determining compliance by performing the following:</p> <ol style="list-style-type: none"> 1. Review site's physical security policy. 2. Verify that users are informed of this policy by reviewing user agreement, posted signs, or training material. 3. Powering off, removal of batteries or blocking IR ports is not acceptable for disabling camera functionality, as this method has not been tested for efficacy. 4. Mark as a finding if a written policy and user training does not prohibit these devices in classified areas. 						
Comments:						
Open		Not a Finding		Not Reviewed		Not Applicable

WIR1010 Establish CMI procedures for Wireless PEDs and systems.

CAT II	WIR1010	V0011820	MAC: 1, 2, 3	CL: C, S	IAC: PRTN-1, VIIR-1, VIIR-2	Ref: DoDD 8530.2
Vulnerability: Wireless email device classified incident handling is not compliant.						
The IAO will ensure that if a Classified Message Incident (CMI) occurs on a Sensa Windows Mobile device or system, the following actions are completed.						
<u>For Apriva Sensa system</u>						
In accordance with DoD policy, all components must establish Incident Handling and Response procedures. A CMI or "data spill" occurs when a classified e-mail is inadvertently sent on an unclassified network and received on a Windows Mobile device. Windows Mobile devices with Sensa are not authorized for processing classified data.						
<ul style="list-style-type: none"> – The Sensa Management and Mail server(s) and Microsoft Exchange server(s) are handled as classified systems until they are sanitized according to appropriate procedures. – The Windows Mobile PDA is handled as a classified device and must be destroyed according to DoD guidance for destroying classified equipment. Currently, there is no reliable method for sanitizing Windows Mobile handhelds after a CMI. 						
Check:						
<ol style="list-style-type: none"> 1. Interview the IAO. 2. Verify classified incident handling, response, and reporting procedures are documented and wireless email device users are trained on these requirements (or requirements are listed on signed user agreement). 						
Comments:						
Open		Not a Finding		Not Reviewed		Not Applicable

WIR1020 Do not use wireless e-mail for classified messages.

CAT I	WIR1020	V0014016	MAC: 1, 2, 3	CL: C	IAC: ECWN-1	Ref: DoDD 8100.2
Vulnerability: Wireless e-mail devices are used for classified.						
The IAO will ensure wireless two-way email devices and systems are not used to send, receive, store, or process classified messages.						
Check: Interview the IAO. Verify local written policy and user training (or requirement listed on signed user agreement) on this requirement.						
Mark as a finding if users are not informed of this policy through training, user agreement, or posted signs.						
Comments:						
Open		Not a Finding		Not Reviewed		Not Applicable

WIR1040 Do not connect wireless e-mail to classified computers.

CATI	WIR1040	V0011832	MAC: 1, 2, 3	CL: C	IAC: ECWN-1	Ref: DoDD 8100.2
Vulnerability: Wireless e-mail devices are connected to a classified network.						
The IAO will ensure that wireless e-mail and systems are not connected to classified DoD networks or information systems.						
Check: <ol style="list-style-type: none">If possible, work with the traditional security reviewer to determine compliance.						
<u>For Apriva Sensa system</u> <ol style="list-style-type: none">Verify written policy and training material exists (or requirement listed on signed user agreement) that states that either wireless devices or specifically Sensa devices must not be connected directly or indirectly (hot synced) to classified computers or networks.						
Comments:						
Open		Not a Finding		Not Reviewed		Not Applicable

2.2 Unclassified Information

WIR0010 All wireless systems must have DAA approval.

CAT I	WIR0010	V0008283	MAC: 1, 2, 3	CL: S, P	IAC: ECWN-1	Ref: DoDD 8100.2
Vulnerability: Use of unauthorized wireless devices and software.						
<p>The IAO will ensure all wireless systems (including associated peripheral devices, operating system, applications, network/PC connection methods, and services) are approved by the DAA prior to installation and used for processing DoD information.</p> <p>Check: Work with the site point-of-contact (POC) to verify documentation. Must be performed with WIR0016 (equipment list) as follows:</p> <ol style="list-style-type: none"> 1. Request copies of written DAA approval documentation: <ul style="list-style-type: none"> – A signed wireless inventory list, SSAA, or DAA approval documents as proof of compliance. – DAA approval letter and SSAA may be a general statement of approval rather than list each device. 2. If site does not have a complete list of wireless equipment, the reviewer may use the <i>SRR Worksheets</i> in the <i>Wireless Security Checklist, Appendix B SRR Worksheets</i> to interview the SA and record equipment details. 3. Verify DAA approval for each device used (i.e., wireless connection services, peripherals, and applications). <p>Mark this check as a finding for any of the following reasons:</p> <ul style="list-style-type: none"> – Wireless systems, devices, services, or accessories are in use but DAA approval letter (s) do not exist – If in the judgment of the reviewer, configuration differs significantly from that approved by the DAA approval letter. 						
Comments:						
Open		Not a Finding		Not Reviewed		Not Applicable

WIR0011 Personally owned PEDs need DAA approval and forfeiture agreement.

CAT III	WIR0011	V0014025	MAC: 1, 2, 3	CL: S, P	IAC: ECSC-1	Ref: Wireless STIG
Vulnerability: Personally owned devices will not be used.						
<p>The IAO will ensure personally owned PEDs are not used to transmit, receive, store, or process DoD information unless approved by the DAA, the owner signs forfeiture agreement in case of a security incident.</p> <p>Check: Interview the IAO as follows:</p> <ol style="list-style-type: none"> 1. Ask if users are using personally owned devices (such as PDAs, Blackberries, laptops, or home computers) to access sensitive Enclave resources. Access to publicly available resources in the Demilitarized Zone (DMZ) can be accessed via personal devices, depending on the INFOCON level. 2. If personally owned devices are allowed, verify written DAA approval exists and the System Security Authorization Agreement (SSAA) is annotated. 3. Verify remote user agreement (including forfeiture agreement) or training material is used to train users on security this requirement. 4. Mark as a finding if: <ul style="list-style-type: none"> – CAT I finding if personally owned devices are used for classified access. – CAT III finding if forfeiture agreement or training is not part of site's procedure or if users are allowed to use personally owned PEDs without DAA approval. <p>Hint: This check includes any non-DoD owned or approved devices such as computers, PEDs/PDAs, and wireless Network Interface Cards (NICs). This applies to administrative and end user access. Use for end user is discouraged but may be approved by DAA.</p>						
Comments:						
Open		Not a Finding		Not Reviewed		Not Applicable

WIR0012 Display required DoD logon banner on PDA.

CAT II	WIR0016	V00015399	MAC: 1, 2, 3	CL: S, P	IAC: DCHW-1	Ref: DoD CIO Memo, 2 Nov 2007
Vulnerability: DoD Logon Banner not displayed.						
<p>The IAO will ensure all PDAs display the following banner during device unlock/logon:</p> <p>A. Use this banner for desktops, laptops, and other devices accommodating banners of 1300 characters. The banner shall be implemented as a click-through banner at logon (to the extent permitted by the operating system), meaning it prevents further activity on the information system unless and until the user executes a positive action to manifest agreement by clicking on a box indicating "OK."]</p> <p>You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.</p> <p>By using this IS (which includes any device attached to this IS), you consent to the following conditions:</p> <p>-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.</p>						

-At any time, the USG may inspect and seize data stored on this IS.
-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.
-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.
-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

B. For Blackberries and other PDAs/PEDs with severe character limitations:]
I've read & consent to terms in IS user agreem't.

Check:

For the Apriva Sensa system

Work with the SA to review the configuration of the Trust Digital server. Reviewed as part of WIR1250 check.

Comments:

Open		Not a Finding		Not Reviewed		Not Applicable	
------	--	---------------	--	--------------	--	----------------	--

WIR0016 Maintain an equipment list of all approved wireless devices.

CAT III	WIR0016	V0008284	MAC: 1, 2, 3	CL: S, P	IAC: DCHW-1	Ref: DoDD 8100.2
Vulnerability: Wireless equipment list not available/updated						
The IAO will maintain a list of all DAA approved wireless devices. The list will be stored in a secure location.						
Check: : 1. Verify existence of site wireless equipment list. 2. Determine process for updating list. and keeping it current. List should indicate date of last update.						
Comments:						
Open		Not a Finding		Not Reviewed		Not Applicable

WIR0030 Document equipment in the SSP

CAT III	WIR0030	V0008297	MAC: 1, 2, 3	CL: S, P	IAC: EBCR-1	Ref: Wireless STIG
Vulnerability: SSAA is not established or properly updated.						
The IAO will ensure wireless devices connecting directly or indirectly (e.g., hotsync, ActiveSync, wireless) to the network are added to the site System Security Plan (SSP).						
Check: Review the SSP for the following: 1. Wireless network devices such as access points, laptops, PEDs, and wireless peripherals (e.g., keyboards, pointers, etc.) that use a wireless network protocol such as Bluetooth, 802.11, or proprietary protocols must be documented in the SSP. 2. A general statement in the SSP permitting the various types of wireless network devices used by the site is acceptable rather than a by-model listing (e.g., a statement that “wireless devices of various models are permitted but only when configured in accordance with the Wireless STIG or other such specified restriction”). 3. Mark as a finding if a DAA approved SSP does not exist or if it is not updated.						
Comments:						
Open		Not a Finding		Not Reviewed		Not Applicable

WIR0072 Wireless network devices must be physically protected.

CAT II	WIR0072	V0014894	MAC: 1, 2, 3	CL: C, S	IAC: PEPF-1, PEPF-2	Ref: DoDI 8500.2 NSA SECNET 11 CONOPS
Vulnerability: Communications devices not physically secured						
The Network Security Officer (NSO) will ensure all network devices (i.e., Intrusion Detection System [IDS], routers, servers, Remote Access System [RAS], firewalls, wireless local area network [WLAN] access points, etc.) are located in a secure room with limited access or otherwise secured to prevent tampering or theft.						
Check: Work with the traditional security reviewer to verify as follows: 1. During SRR walkthrough inspection, visually confirm that wireless APs, Video, Voice over IP (VoIP), IDS, and other network components are installed in secured areas. 2. Mark as a finding if wireless network hardware is not physically secured as required.						
Comments:						
Open		Not a Finding		Not Reviewed		Not Applicable

WIR0076 Require signed user agreement.

CAT III	WIR0076	V0014020	MAC: 1, 2, 3	CL: S	IAC: PRTN-1	Ref: Wireless STIG
Vulnerability: User agreement is not compliant						
For mobile and remote users of the DoD enclave and resources, the IAM will develop a written security policy or checklist for secure wireless remote access to the site and an agreement between the site and remote user.						
DoD CIO Memorandum "Policy on Use of Department of Defense (DoD) Information Systems Standard Consent Banner and User Agreement," dated 9 May 2008 requires the following additional information in all User Agreements:						
<i>STANDARD MANDATORY NOTICE AND CONSENT PROVISION FOR ALL DOD INFORMATION SYSTEM USER AGREEMENTS By signing this document, you acknowledge and consent that when you access Department of Defense (DoD) information systems:</i>						
You are accessing a U.S. Government (USG) information system (IS) (which includes any device attached to this information system) that is provided for U.S. Government authorized use only.						
You consent to the following conditions:						
<ul style="list-style-type: none"> – The U.S. Government routinely intercepts and monitors communications on this information system for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations. – At any time, the U.S. Government may inspect and seize data stored on this information system. – Communications using, or data stored on, this information system are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any U.S. Government-authorized purpose. 						

- This information system includes security measures (e.g., authentication and access controls) to protect U.S. Government interests--not for your personal benefit or privacy.
- Notwithstanding the above, using an information system does not constitute consent to personnel misconduct, law enforcement, or counterintelligence investigative searching or monitoring of the content of privileged communications or data (including work product) that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Under these circumstances, such communications and work product are private and confidential, as further explained below:
 - Nothing in this User Agreement shall be interpreted to limit the user's consent to, or in any other way restrict or affect, any U.S. Government actions for purposes of network administration, operation, protection, or defense, or for communications security. This includes all communications and data on an information system, regardless of any applicable privilege or confidentiality.
 - The user consents to interception/capture and seizure of ALL communications and data for any authorized purpose (including personnel misconduct, law enforcement, or counterintelligence investigation). However, consent to interception/capture or seizure of communications and data is not consent to the use of privileged communications or data for personnel misconduct, law enforcement, or counterintelligence investigation against any party and does not negate any applicable privilege or confidentiality that otherwise applies.
 - Whether any particular communication or data qualifies for the protection of a privilege, or is covered by a duty of confidentiality, is determined in accordance with established legal standards and DoD policy. Users are strongly encouraged to seek personal legal counsel on such matters prior to using an information system if the user intends to rely on the protections of a privilege or confidentiality.
 - Users should take reasonable steps to identify such communications or data that the user asserts are protected by any such privilege or confidentiality. However, the user's identification or assertion of a privilege or confidentiality is not sufficient to create such protection where none exists under established legal standards and DoD policy.
 - A user's failure to take reasonable steps to identify such communications or data as privileged or confidential does not waive the privilege or confidentiality if such protections otherwise exist under established legal standards and DoD policy. However, in such cases the U.S. Government is authorized to take reasonable actions to identify such communication or data as being subject to a privilege or confidentiality, and such actions do not negate any applicable privilege or confidentiality.
 - These conditions preserve the confidentiality of the communication or data, and the legal protections regarding the use and disclosure of privileged information, and thus such communications and data are private and confidential. Further, the U.S. Government shall take all reasonable measures to protect the content of captured/seized privileged communications and data to ensure they are appropriately protected.
- In cases when the user has consented to content searching or monitoring of communications or data for personnel misconduct, law enforcement, or counterintelligence investigative searching, (Le., for all communications and data other than privileged communications or data that are related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants), the U.S. Government may, solely at its discretion and in accordance with DoD policy, elect to apply a privilege or other restriction on the U.S. Government's otherwise-authorized use or disclosure of such information.

-
- All of the above conditions apply regardless of whether the access or use of an information system includes the display of a Notice and Consent Banner ("banner"). When a banner is used, the banner functions to remind the user of the conditions that are set forth in this User Agreement, regardless of whether the banner describes these conditions in full detail or provide a summary of such conditions, and regardless of whether the banner expressly references this User Agreement.

DoD sites should consider adding the following information to site User Agreements:

- The agreement should contain the type of access required by the user (privileged, end-user, etc.).
- The agreement should contain the responsibilities, liabilities, and security measures (e.g., malicious code detection training) involved in the use of the wireless remote access device.
- Incident handling and reporting procedures will be identified along with a designated point of contact.
- The remote user can be held responsible for damage caused to a Government system or data through negligence or a willful act.
- The policy should contain general security requirements and practices, which are acknowledged and signed by the remote user.
- If classified devices are used for remote access from an alternative work site, the remote user will adhere to DoD policy in regard to facility clearances, protection, storage, distributing, etc.
- Government owned hardware and software is used for official duties only. The employee is the only individual authorized to use this equipment.

Check: Ensure the following:

1. Inspect a copy of the site's user agreement.
2. Verify user agreement has the minimum elements described in the STIG policy.
3. User agreements are particularly important for mobile and remote users since there is a high risk of loss, theft, or compromise thus, this signed agreement is a good best practice to help ensure the site is making the user is aware of the risks and proper procedures.

Mark as a finding if site user agreements do not exist or are not compliant with the minimum requirements.

Comments:

Open		Not a Finding		Not Reviewed		Not Applicable	
------	--	---------------	--	--------------	--	----------------	--

WIR0371 PEDs with cameras must be approved by physical security policies.

CAT III	WIR0371	V0004840	MAC: 1, 2, 3	CL: S, P	IAC: ECWN-1	Ref: DoDD 8100.2
Vulnerability: PED camera policy does not exist						
<p>The IAO will ensure PEDs with digital cameras (still and video) are allowed in a DoD facility only if specifically approved by site physical security policies.</p> <p>Check: Review site's physical security policy. Verify that it addresses PED devices with embedded cameras.</p> <p>Mark this as a finding if there is no written physical security policy outlining whether wireless phones with cameras are permitted or prohibited on or in this DoD facility.</p>						
Comments:						
Open	<input type="checkbox"/>	Not a Finding	<input type="checkbox"/>	Not Reviewed	<input type="checkbox"/>	Not Applicable

WIR1015 Establish disposal procedures for Sensa Wireless PEDs and systems.

CAT III	WIR1015	V0014938	MAC: 1, 2, 3	CL: C, S	IAC: PRTN-1, VIIR-1, VIIR-2	Ref: DoDD 8530.2
Vulnerability: Disposal of Wireless e-mail device is not compliant.						
<p>The IAO will ensure that prior to disposing of a wireless e-mail handheld PED (e.g., sold, transferred to another DoD or other government agency, etc.), the procedures found in the appropriate wireless push e-mail system checklist are followed.</p> <p><u>For Windows Mobile handhelds</u></p> <p>The handheld manufacturer's procedure must be followed to wipe all user/application addressable memory and return the device and all memory to factory default status.</p> <p>Check: Interview the IAO. Verify proper procedures are being followed and the procedures are documented.</p>						
Comments:						
Open			Not a Finding		Not Reviewed	Not Applicable

WIR1080 Install Wireless e-mail servers using an approved architecture.

CAT I	WIR1080	V0014022	MAC: 1, 2, 3	CL: S, P	IAC: ECSC-1	Ref: Wireless STIG
Vulnerability: Network architecture is not compliant						
<p>The IAO will ensure that the wireless e-mail system is set up with the required system components and software installed on the handheld device.</p> <p>Check: Interview the IAO and SA and review system network diagrams.</p> <p><u>For Apriva Sensa system</u></p> <p>Verify that all system components listed in Section 3.2 of this checklist are being used:</p> <ul style="list-style-type: none"> – Apriva Sensa Management Server (version 1.9.2 or later) – Apriva Sensa Mail Server (version 1.9.2 or later) – Mobile Device Security Policy Manager that centrally manages all devices via an enterprise installed management server (Trust Digital 7.3 or later) – Windows Mobile compatible PDA or smartphone with the following software: <ul style="list-style-type: none"> a. Windows Mobile 5.0 (or 6.0 when Trust Digital supports this version) b. Apriva Sensa client c. Security Policy Management client (Trust Digital) d. DoD approved mobile device anti-virus application e. Mobile device personal firewall (Trust Digital) – Apriva BT100-C or BT200 Bluetooth Smart Card Reader – Microsoft Exchange 2003, Service Pack (SP) 2 (earlier versions of Microsoft Exchange and Microsoft Exchange 2007 may not be used; required security features are not available) – Microsoft Exchange ActiveSync – Microsoft Active Directory Domain Controller 2003 SP1 or SP2 – Enclave Firewall 						
Comments:						
Open		Not a Finding		Not Reviewed		Not Applicable

WIR1090 Required actions if Wireless e-mail handheld is lost or stolen.

CAT II	WIR1090	V0003544	MAC: 1, 2, 3	CL: S, P	IAC: ECSC-1	Ref: Wireless STIG
Vulnerability: Wireless e-mail devices are not deactivated if lost/stolen.						
<p>The IAO will ensure the wireless e-mail system administrator (SA) sends a “Wipe” or “Kill” command to the device and removes the device from the wireless e-mail management server when a wireless e-mail device is reported lost or stolen.</p> <p>If a wireless e-mail device is lost or stolen, the device must be immediately disabled to prevent unauthorized use or access. Once the device is deemed unrecoverable, the device should be permanently removed from the server and SA should contact the service provider to cancel the service.</p> <p>Check: <u>For Apriva Sensa system</u></p> <p>The Sensa administrator will follow one on the following two procedures:</p> <p><u>Procedure 1</u></p> <ol style="list-style-type: none"> 1. Log into the Sensa Management Server. 2. Choose Mail Server Enclave. 3. Select Accounts for enclave device is registered under. 4. Scroll to device of interest, then select Remove under user Account Name. 5. Click Yes to remove account and zeroize device. <p><u>Procedure 2</u></p> <ol style="list-style-type: none"> 1. Log into the Trust Digital Enterprise Console. 2. Select Help Desk Tab. 3. Search for user whose device needs to be wiped. 4. Select device to wipe. 5. Click on Wipe. <p>Interview the IAO. Review written policies and end user training materials. Verify that proper procedures are followed when devices are lost or stolen.</p>						
Comments:						
Open		Not a Finding		Not Reviewed		Not Applicable

WIR1100 Authenticated login procedures to unlock a wireless e-mail device.

CAT II	WIR1100	V0003545	MAC: 1, 2, 3	CL: S, P	IAC: ECSC-1	Ref: Wireless STIG
Vulnerability: Wireless e-mail device not protected by authentication.						
The IAO will ensure the wireless e-mail device is protected by authenticated login procedures to unlock the device. Either Common Access Card (CAC) or Personal Identification Number (PIN) authentication is required.						
When PIN authentication is used, the following procedures will be enforced:						
<ul style="list-style-type: none"> – The device password /PIN is set to five or more characters. The system security policy must be configured to enforce this policy. If five characters are used, both a letter (lower or upper case) and a number must be used in all device passwords (the wireless email server must be configured to enforce this policy). If six or more characters are used, only numbers may be used for the password. It is recommended that eight or more characters be used. – The number of incorrect passwords entered before a device wipe occurs is set to 10 or less. The system security policy must be configured to enforce this policy. – The password is changed at least every 90 days. The system security policy must be configured to enforce this policy. 						
Check: Interview the IAO and administrator for the following:						
<ol style="list-style-type: none"> 1. Verify CAC authentication or PIN authentication is used. 2. If PIN authentication is used, verify correct settings. These policies are given in Appendix B and are reviewed as part of check WIR1250. The reviewer must raise this to a CAT I finding if any configuration setting designated as CAT I remains in an Open status. The reviewer should lower to a CAT III if only configuration settings designated as CAT III remain in an Open status. 						
Comments:						
Open		Not a Finding		Not Reviewed		Not Applicable

WIR1120 Wireless e-mail handhelds are set to lock after no more than 15 minutes of inactivity.

CAT II	WIR1120	V0007077	MAC: 1, 2, 3	CL: S, P	IAC: ECSC-1	Ref: Wireless STIG
Vulnerability: Wireless e-mail device not set for a 15-minute lockout						
The IAO will ensure all Windows Mobile handhelds with Sensa are set to lock (timeout) after no more than 15 minutes of inactivity.						
Check:						
<u>For Apriva Sensa system</u>						
Work with the SA to review the configuration of the Sensa Management Server policy rules. Reviewed as part of WIR1250 check.						
Comments:						
Open		Not a Finding		Not Reviewed		Not Applicable

WIR1140 Bluetooth usage must be compliant.

CAT II	WIR1140	V0014198	MAC: 1, 2, 3	CL: S, P	IAC: ECSC-1	Ref: Wireless STIG
Vulnerability: Wireless e-mail device Bluetooth configuration not compliant						
<p>The IAO will ensure a wireless e-mail device, which has a Bluetooth radio, applies the following Bluetooth controls:</p> <ul style="list-style-type: none"> Bluetooth data transmissions (e.g., syncing to the desktop or transfer of data files) on wireless e-mail devices are disabled except for the Bluetooth CAC reader (i.e., Bluetooth Smart Card Reader [SCR]). Only DISA tested and approved Bluetooth SCRs may be used. Bluetooth for voice transmissions (e.g., Bluetooth ear bud) is not authorized. Both the Bluetooth Handsfree and Headset profiles must be disabled. Users should use wired hands-free devices. <p>Check: <u>For Apriva Sensa systems</u></p> <p>Perform the following checks on a sample of handheld devices:</p> <ol style="list-style-type: none"> Verify the Bluetooth icon/app is not available. On the handheld, go to Start/Settings/Connections. Verify that Bluetooth cannot be turned on by the user. <ul style="list-style-type: none"> On the handheld, go to Start/Settings/Connections/then open the Wireless Manager/then select Menu/then select Bluetooth Setting and see that nothing happens 						
Comments:						
Open		Not a Finding		Not Reviewed		Not Applicable

WIR1150 Bluetooth Smart Card Reader usage must be compliant.

CAT III	WIR1150	V0011866	MAC: 1, 2, 3	CL: S, P	IAC: ECSC-1	Ref: Wireless STIG
Vulnerability: Wireless e-mail device Bluetooth SCR usage not compliant						
<p><u>For Apriva Sensa system</u></p> <p>The IAO will ensure that only the Apriva BT100-C or BT200 Bluetooth SCRs are used with Windows Mobile devices using Sensa e-mail.</p> <p>Check: Interview the IAO and administrator. Verify that only approved Bluetooth smart card readers are used.</p>						
Comments:						
Open		Not a Finding		Not Reviewed		Not Applicable

WIR1160 Secure wireless e-mail servers using operating system STIG.

CAT II	WIR1160	V0014199	MAC: 1, 2, 3	CL: S, P	IAC: ECSC-1	Ref: Wireless STIG
Vulnerability: Operating system for wireless e-mail server host is not compliant.						
<u>For Apriva Sensa system</u>						
The IAO will ensure that all host servers and computers where Sensa services are installed (e.g., Sensa Management server, Sensa Mail server, Exchange e-mail server, and Lightweight Directory Access Protocol [LDAP] server) are hardened in accordance with the appropriate operating system (OS) STIG.						
Check: Work with the OS reviewer or check VMS for last review of the host computer asset. Verify that there are not outstanding CAT I findings associated with the host server.						
Mark as a finding if CAT I findings are open for the host computer operating system or if a SRR or site self-check was not performed for the host computer.						
Comments:						
Open		Not a Finding		Not Reviewed		Not Applicable

WIR1170 Comply with provisioning requirements for new/re-issued wireless e-mail devices.

CAT II	WIR1170	V0011868	MAC: 1, 2, 3	CL: S, P	IAC: ECSC-1	Ref: Wireless STIG
Vulnerability: Wireless e-mail devices wipe procedures are not compliant						
The IAO will ensure that a wireless e-mail SA performs a "Device HARD Reset" on all new or reissued wireless e-mail devices and that all system software is reloaded on the device from a trusted source and the site security policy is pushed to the device before issuing it to DoD personnel and placing the device on a DoD wireless e-mail network.						
<u>For Apriva Sensa system</u>						
If Over-the-Air (OTA) provisioning is used, the following steps must be followed by the system administrator:						
<ul style="list-style-type: none"> – Windows Mobile device users are not allowed to wirelessly activate their Windows Mobile device unless under the direction of the SA. – Provide the Windows Mobile device user provisioning instructions and the Trust Digital Portal Uniform Resource Locator [URL] by a secure method (e.g., via signed and encrypted e-mail) to desktop PC/laptop. – Only the SA has admin rights to the provisioning portal and can load software on the portal for download. 						
Check: Interview the IAO. Verify required procedures are followed.						
Comments:						
Open		Not a Finding		Not Reviewed		Not Applicable

WIR1180 Do not allow users to install or remove applications.

CAT I	WIR1180	V0011869	MAC: 1, 2, 3	CL: S, P	IAC: ECSC-1	Ref: Wireless STIG
Vulnerability: Users allowed to update or remove applications						
The IAO will ensure that wireless e-mail users do not install or remove applications and/or software on their handheld device unless under the direction and supervision of an authorized Sensa SA.						
Check: Work with the wireless e-mail SA to verify this requirement by reviewing the following:						
<u>For Apriva Sensa system</u>						
Check the Policy settings of the Trust Digital policy. Reviewed as part of WIR1250 check.						
Comments:						
Open		Not a Finding		Not Reviewed		Not Applicable

WIR1200 Digitally sign emergency and/or critical e-mail notifications.

CAT II	WIR1200	V0011871	MAC: 1, 2, 3	CL: S, P	IAC: ECSC-1	Ref: Wireless STIG
Vulnerability: Emergency or critical messages not signed						
The IAO will ensure that all emergency and/or critical e-mail notifications are digitally signed and verified to ensure the authenticity of the sender.						
Check: Interview the IAO.						
<u>For Apriva Sensa systems</u>						
<ol style="list-style-type: none"> 1. Verify that Secure Multipurpose Internet Mail Extensions (S/MIME) is configured such that users may sign messages. 2. Check a sample of Sensa devices: <ul style="list-style-type: none"> – Verify Sensa client is installed on the device. Go to Start/Programs/verify Sensa icon is present. – Verify DoD Root certificates are configured on the device: Go to Start/Settings/System/Certificates/Root. 3. Verify that users are trained on how to sign messages on the Sensa handheld and that users are trained to sign emergency and critical e-mail notifications. 						
Comments:						
Open		Not a Finding		Not Reviewed		Not Applicable

WIR1210 Configure wireless email auto signature as required.

CAT III	WIR1210	V0011872	MAC: 1, 2, 3	CL: S, P	IAC: ECSC-1	Ref: Wireless STIG
Vulnerability: Signature message is not compliant						
<p>The IAO will ensure that if wireless e-mail auto signatures are used and that signature message does not disclose that the e-mail originated from a mobile device (e.g., "Sent From My Windows Mobile Wireless Handheld").</p> <p>Check: Check a sample of devices to verify auto signature meets the requirement.</p> <p><u>For Apriva Sensa system</u></p> <p>On the handheld, launch the Sensa Mail Client/select Menu/select Options/select General tab/view signature in text box.</p> <p>Comments:</p>						
Open		Not a Finding		Not Reviewed		Not Applicable

WIR1220 If Text Messaging is used, enable security.

CAT II	WIR1220	V0011873	MAC: 1, 2, 3	CL: S, P	IAC: ECSC-1	Ref: Wireless STIG
Vulnerability: Text Messaging is not configured to use S/MIME.						
<p>The IAO will ensure security requirements for text messaging (such as, Short Message Service [SMS], Multimedia Messaging Service [MMS], Pin-to-Pin messaging, and other text messaging services) are followed as described in the appropriate wireless e-mail system checklist.</p> <p>If SMS is used, annual Information Assurance (IA) awareness training must include security threats of SMS and MMS.</p> <p>If SMS is not used, it must be disabled with the system security policy and wireless service contracts should not include text messaging services.</p> <p>Check: <u>For Apriva Sensa system</u></p> <ol style="list-style-type: none"> 1. Determine if SMS/MMS is enabled: Launch the Trust Digital Management Console. Select Policy Manager>Resource Settings. 2. If SMS is used, interview the IAO and check IA awareness training material to ensure training includes SMS/MMS security issues. 3. If SMS is not used, interview the telephone office to verify wireless service plans do not contain text messaging services. <p>Comments:</p>						
Open		Not a Finding		Not Reviewed		Not Applicable

WIR1250 Implement wireless e-mail servers and handheld configuration settings.

CAT II	WIR1250	V0011876	MAC: 1, 2, 3	CL: S, P	IAC: ECSC-1	Ref: Wireless STIG
Vulnerability: The wireless e-mail server and handheld device configurations are not compliant						
<p>The IAO will ensure that all required wireless e-mail servers and device configuration settings are implemented.</p> <p><u>For Apriva Sensa system</u></p> <p>See requirements listed in Section 3 and Appendix B.</p> <p>Check: <u>For Apriva Sensa system</u></p> <ol style="list-style-type: none"> 1. Verify the Certificate Store password meets requirements listed in section 3.3 based on current INFOCON level. Interview the Sensa SA for the following: <ul style="list-style-type: none"> – Ensure proper passwords are being used: <ul style="list-style-type: none"> ○ Have SA restart Sensa System Attendent. ○ Check passwords that SA enters to start Mail Server and Management Server and ensure they meet requirements listed in section 3.4 of this checklist. – Ensure passwords are recorded and stored in a secure manner. 2. Verify the Sensa Admin accounts are configured to meet requirements listed in section 3.4 based on current INFOCON level. Interview the Sensa SA and have them show you the current settings. Check for the following: <ul style="list-style-type: none"> – Verify separate admin accounts are set up for each administrative user: <ul style="list-style-type: none"> ○ Interview the SA and ensure proper passwords are being used. ○ Ensure passwords are recorded and stored in a secure manner. – Verify the password on a sample of admin accounts meets requirements listed in 3.8. – Verify the default admin account has been deleted. 3. Verify the Trust Digital Admin accounts are configured to meet requirements listed in section 3.4 based on current INFOCON level. Interview the Sensa SA and have them show you the current setting. Check for the following: <ul style="list-style-type: none"> – Verify separate admin accounts are set up for each administrative user: <ul style="list-style-type: none"> ○ Interview the Sensa SA and ensure proper passwords are being used. ○ Ensure passwords are recorded and stored in a secure manner. 4. Verify the password on a sample of admin accounts meets requirements listed in 3.4 5. Verify all required Sensa policy settings listed in Table B1 are set. Have the Sensa SA show you the current policy settings. Launch Sensa Management Server/Select Mail Server Enclave for enclave being managed/Select Policies/For policy being reviewed, select View. 						

6. Verify all required Trust Digital policy settings listed in Table B2 are set. Have the Sensa SA show you the current policy settings: Launch the Trust Digital Management Console, and select the appropriate management tab.
7. Verify all required Symantec configuration settings listed in Table B3 are set. Have the Sensa SA show you the current policy settings: On **Today** screen of handheld, tap **Symantec** icon on bottom right corner, and select **Open Symantec Antivirus**.
8. Verify written policy and training material exists (or requirement listed on signed user agreement) that states that user must manually download new virus definition files and perform scan at least once every week.

The reviewer must raise this to a CAT I finding if **any** configuration setting designated as CAT I **remains in an Open status**. The reviewer should lower to a CAT III **if only** configuration settings designated as CAT III **remain in an Open status**.

Note: Open checks in Appendix B should be marked against the check number listed in the table for the "Open" IT Policy rule.

Comments:

Open	<input type="checkbox"/>	Not a Finding	<input type="checkbox"/>	Not Reviewed	<input type="checkbox"/>	Not Applicable	<input type="checkbox"/>
------	--------------------------	---------------	--------------------------	--------------	--------------------------	----------------	--------------------------

WIR1280 Data-at-rest encryption is enabled on all wireless e-mail devices.

CAT III	WIR1280	V0012164	MAC: 1, 2, 3	CL: S	IAC: ECSC-1	Ref: Wireless STIG
----------------	---------	----------	--------------	-------	-------------	--------------------

Vulnerability: Data-at-Rest encryption is not enabled

The IAO will ensure Data-at-Rest encryption is enabled on all wireless push e-mail handheld devices.

Check:

Work with SA to verify that data-at-rest encryption is set as required. Checked as part of WIR1250 check.

Note: Encryption must be FIPS 140-2 certified (verified during DISA system testing).

Comments:

Open	<input type="checkbox"/>	Not a Finding	<input type="checkbox"/>	Not Reviewed	<input type="checkbox"/>	Not Applicable	<input type="checkbox"/>
------	--------------------------	---------------	--------------------------	--------------	--------------------------	----------------	--------------------------

3. SENA SECURITY RELATED CONFIGURATIONS

3.1 Known System Limitations

Table 3-1 lists known system limitations that may impact system performance, usability, supportability, or security of the Sensa system.

Issue	Comments
User cannot use their CAC to authenticate to Web sites.	Fix expected in a future Sensa release.
User must authenticate twice when unlocking the handheld device.	The Sensa client is used as the primary system for handheld access control (requires CAC authentication). The Trust Digital password protection cannot be disabled, but it can be set to single digit.
When Pocket Internet Explorer (PIE) is configured to connect to a DoD Web-proxy, a Secure Sockets Layer (SSL) connection cannot be established for secure user authentication to the proxy.	Limitation of PIE. There is not a setting in PIE to use a secure connection between PIE and the proxy server to secure the login. (SSL connections to Web sites are available.)
Trust Digital Firewall has no logging capability.	

Table 3-1: Known Sense System Limitations

3.2 Sensa System Architecture

The Apriva Sensa secure mobile e-mail system consists of the following components:

- Apriva Sensa Management Server (version 1.9.2 or later)
- Apriva Sensa Mail Server (version 1.9.2 or later)
- Mobile Device Security Policy Manager that centrally manages all devices via an enterprise installed management server
- Windows Mobile compatible PDA or smartphone with the following software:
 - o Windows Mobile 5.0 (Sensa supports WM 6.0 and Trust Digital will support WM 6.0 in the near future)
 - o Apriva Sensa client
 - o Security Policy Management client
 - o DoD approved mobile device anti-virus application
 - o Mobile device personal firewall
- Apriva BT100-C or BT200 Bluetooth SCR
- Microsoft Exchange 2003, SP2 (earlier versions of Microsoft Exchange and Microsoft Exchange 2007 may not be used; required security features are not available)

Additional network components are required for system operation:

- Enclave Firewall
- Microsoft Active Directory Domain Controller, Microsoft Server 2003 SP1 or later

The Mobile Device Security Policy Manager is required because Apriva Sensa does not have all security policy features that are required for DoD wireless email devices. In addition, anti-virus and/or personal firewall applications may be required if these functions are not included in the Mobile Device Security Policy Manager product selected for the system. For the development of this checklist, the following additional components were added to the Apriva Sensa system:

- Trust Digital version 7.3 (Management of CAC and Password Devices Mode) with the following:
 - o Device Management Gateway
 - o Enterprise Console
 - o Trust Digital Portal and Self-Service Portal
 - o Firewall (this is not a separate component of the TD software)
- Symantec Antivirus for Handhelds (version 3.5)
- Structured Query Language (SQL) Server

DoD sites may substitute other security products for the Trust Digital handheld security policy management server, Trust Digital personal firewall, and Symantec Antivirus application under the following conditions:

- For the alternate security policy management product:
 - o The alternate security policy management product must centrally manage the security policy on all handheld devices.
 - o The alternate security policy management product must provide all features allocated to the Trust Digital product in Table C1, Allocation of DoD Security Requirements to System Components.
 - o The site is responsible for ensuring the interoperability of the selected product with Apriva Sensa.
 - o The site must demonstrate to DISA that all system security requirements are met (or alternately have the system evaluated by an IA authority selected by the DAA and provide DISA FSO a copy of the evaluation report).
 - o The site must provide DISA FSO security configuration instructions for the alternate product similar to the instructions provided for the Trust Digital security policy management product in this checklist.
- For the alternate anti-virus product:

- The alternate anti-virus product must be DoD approved (downloaded from the Joint Task Force - Global Network Operations ([JTF-GNO] anti-virus Web portal).
- The site is responsible for ensuring the interoperability of the selected product with Apriva Sensa and the security policy management product.
- The site must provide DISA FSO security configuration instructions for the alternate product similar to the instructions provided for the Symantec antivirus product in this checklist.
- For the alternate personal firewall product:
 - The firewall shall be able to filter both inbound and outbound traffic based on ports, protocols, services, and Internet Protocol (IP) address.
 - The site is responsible for ensuring the interoperability of the selected product with Apriva Sensa and the security policy management product.
 - The site must provide DISA FSO security configuration instructions for the alternate product similar to the instructions provided for the Trust Digital firewall product in this checklist.

Figure 3-1 shows the recommended system architecture without a Microsoft Internet Security and Acceleration (ISA) Server. The Trust Digital server components have been separated for increased performance and security. Installing all of the Trust Digital services (except for the TD Portal and SelfService Portal) on one server is an acceptable implementation. For this architecture, the TD Portal and SelfService Portal must be installed in the public facing DMZ.

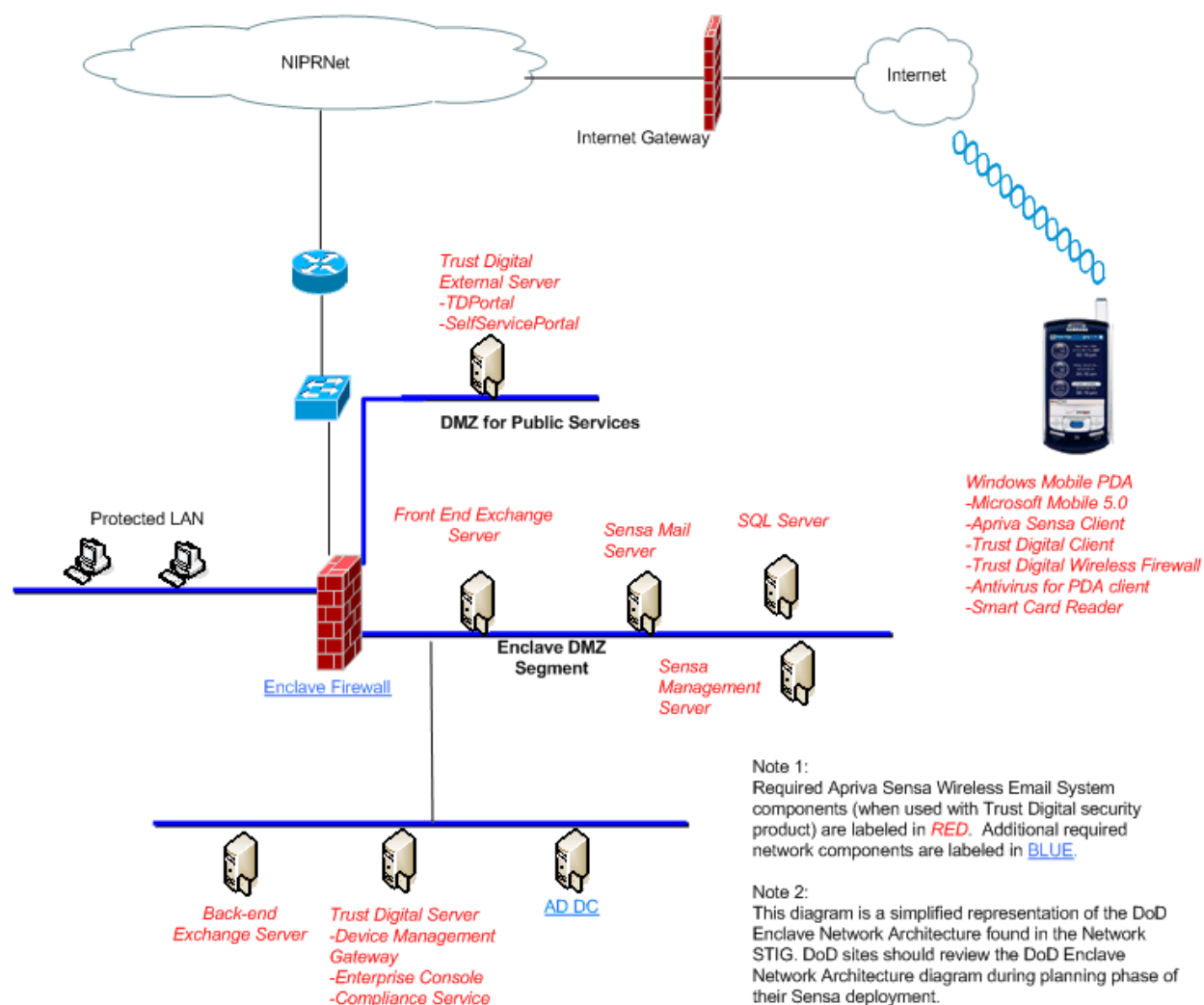


Figure 3-1. Apriva Sensa System Architecture without ISA Server

3.3 Sensa System Setup and Provisioning

This section provide the setup and provisioning information for the Sensa System.

3.3.1 Sensa Server Installation

The Army has developed detailed Sensa system installation instructions in the following document: *Sensa Server Installation*. The *Sensa Server Installation* document can be downloaded from the Army Knowledge Online web portal at <https://www.us.army.mil/suite/doc/8312907>. Apriva documents should also be consulted (see Appendix A).

3.3.2 Windows Mobile Handheld Provisioning

The Army has developed detailed Windows Mobile device with Sensa provisioning instructions in the following document: *Windows Mobile Device Build Procedures*. The *Windows Mobile Device Build Procedures* document can be downloaded from the Army Knowledge Online web portal at <https://www.us.army.mil/suite/doc/8312908>. Apriva documents should also be consulted (see Appendix A).

3.4 Setting Up Certificate Store Password

The Sensa Server Installation Guide provides information on setting up the certificate password during the installation of the Management Server and the Mail Server. This management server password is also the Sensa Management Server data store encryption password. Both of these passwords are used to start the respective servers.

During setup of the Sensa system the following tasks should be completed:

- The certificate passwords should be compliant and maintained IAW DoDI 8500.2 and current JTF-GNO directives.

Note: CAC authentication should be used for all administrative passwords, if this capability is available. When not available, CTO 06-02, 17 January 2006 requires the following for passwords:

- Passwords will be set to a minimum of 9 characters.
- Passwords will contain a mix of at least two lowercase letters, two uppercase characters, two numbers, and two special characters.

In addition, JTF-GNO INFOCON 4 Alert Message, 16 November 2006, requires the following change during INFOCON Level 4:

- Passwords will be set to a minimum of 15 characters.

3.5 Setting Up Certificate Store and Service and Administrative Accounts

This section provides detailed information on setting up certificate store and service and administrative accounts.

3.5.1 Sensa Service Accounts

The *Sensa Server Installation Guide* provides information on setting up a Sensa Service Account on the organization's domain controller. During setup of the Sensa system, the following tasks should be completed:

- The service account password should be compliant and maintained IAW DoDI 8500.2 and current JTF-GNO directives. See Paragraph 3.4 for specific requirements.

3.5.2 Sensa Admin Accounts

The *Sensa System Administration Guide* provides information on setting up Sensa Admin accounts. During setup of the Sensa system, the following tasks should be completed:

- When the local machine login account is generated during the Sensa Management Server installation (sensaAdmin), the password for this account should be compliant and maintained IAW DoDI 8500.2 and current JTF-GNO directives. See Paragraph 3.4 for specific requirements. The default name on the local machine account should be changed. The local machine account should only be used by the Sensa administrator to perform server upgrades, software installs, or critical Sensa maintenance functions.
- DoD Administrative Accounts should implement CAC authentication whenever possible. Apriva supports CAC authentication for the local machine login account.
- Define specific roles for each type of Admin user (launch **SMS**, under **Administration**, select **Roles/Add**, then select only specific functions needed for that role).
- Create individual administrative accounts for each Sensa Admin. (launch **SMS**, under **Administration**, select **Administrative Users/Add**:
 - o The password for this account should be compliant and maintained IAW DoDI 8500.2 and current JTF-GNO directives. See Paragraph 3.4 for specific requirements. To set up password rules for Admin accounts do the following: (launch **SMS**, under **Administration**, select **Security Policies**, select the **Administrator** policy, click **Modify**).
 - o Assign a role to each Admin account. Each account should be given the least permissions required for that job.

3.5.3 Trust Digital Accounts

The *Trust Digital Getting Started Guide* provides information for setting up Admin Accounts for the Trust Digital components.

- Create a SQL database Admin Account during installation of the Trust Digital software. The password for this account should be compliant and maintained IAW DoDI 8500.2 and current JTF-GNO directives. See Paragraph 3.4 for specific requirements.
- After installation of the Trust Digital software, new administrative accounts should be set up for each system administrator. In addition, the default administrative account should be deleted. The password for each administrative account should be compliant and maintained IAW DoDI 8500.2 and current JTF-GNO directives. See Paragraph 3.4 for specific requirements.

NOTE: Trust Digital is expected to add CAC authentication to the Enterprise Console administrative accounts in a future release.

3.6 OCSP Configuration

OCSP provides certificate validation services for all DoD Public Key Infrastructure (PKI) issued certificates in one location. The standard procedure in DoD for validating digital certificates is to query the DoD OCSP rather than downloading and performing a query on a CRL. Configure OCSP on the Sensa server as shown in Figure 3-2.

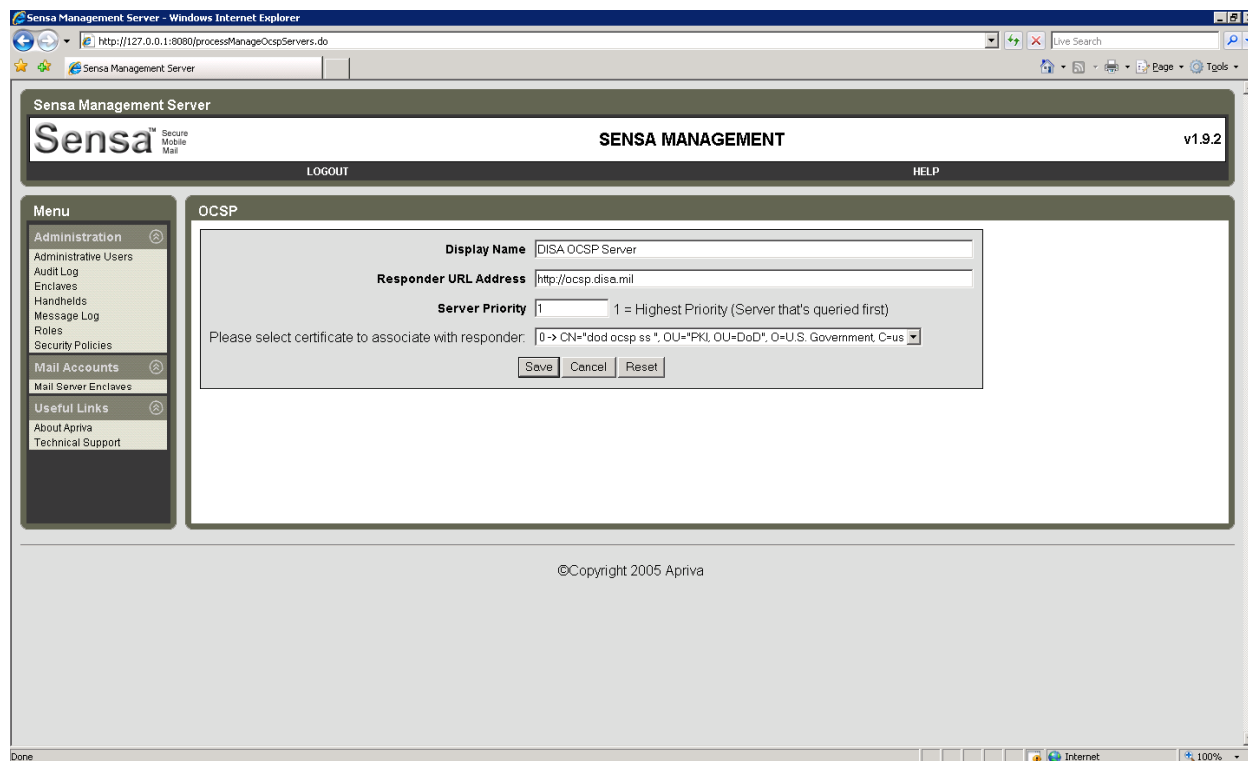


Figure 3-2. OSCP Setup Screen

3.7 Setting up Security Policies

This section provides detailed instructions on how to set up security policies for your Sensa system.

3.7.1 Admin Accounts

The *Sensa System Administration Guide* provides information on setting up security policies for Admin Accounts (launch **SMS**, under **Administration**, select **Security Policies/Add**). The only rules that can be set up for administrators are related to Admin Account password strength and complexity. See Paragraph 3.5.2 for more information.

3.7.2 User Accounts

The *Sensa System Administration Guide* provides information on setting up security policies for Mail Accounts (launch **SMS**, under **Mail Accounts**, under desired **Enclave**, select **Policies**. To create a new policy, select **Add**. See Appendix C for required and optional security policy rule settings.

It is recommended that the Sensa default policy for each **Enclave** be renamed to something like “Factory Default” so that it is available for trouble shooting purposes. Users should not be assigned to the default policy.

3.8 Control of Device Applications

For security reasons, the installation or removal of applications on a handheld device must be strictly controlled. This will ensure malware attached to email or SMS cannot be installed on the PDA or smartphone. Therefore, the **Image Management** policy rule must always be set to **Enabled**. This setting must be turned on after Sensa is installed, or the Sensa install will fail.

3.9 Bluetooth Security Settings

Bluetooth wireless voice and data connections can be established between the Windows Mobile handheld device and any other device with Bluetooth wireless capabilities. There are significant security issues with Bluetooth, therefore, Bluetooth should only be used as follows:

- Voice connection to a Bluetooth earbud cell phone earbud is prohibited due to Bluetooth security issues. Wired handsfree devices should be used.
- Data connections for the Bluetooth smart card reader is the only approved use of Bluetooth (serial port profile only). Only DISA tested and approved Bluetooth Smart Card Readers (i.e., CAC readers) may be used (see section 3.10).

3.10 Bluetooth Smart Card Reader

DoD approved Bluetooth smart card readers (SCR) can be used with DoD wireless e-mail systems. Both the Apriva BT100-C and BT200 Bluetooth SCRs have been tested by National Security Agency (NSA) and have been approved by DISA for use with the Sensa secure mobile e-mail system.

3.11 Enclave Firewall Configuration Requirements

The *Apriva Sensa Server Installation Guide* provides guidance for configuring the enclave firewall to allow required outbound Sensa connections.

Table 3-2 lists the default or standard ports for the needed services. Although it is possible for the site to configure Transmission Control Protocol/User Datagram Protocol (TCP/UDP) to use non-standard or unregistered ports for these communications, this is not recommended as it will cause unexpected results at various internal and external boundaries in the DoD Enclave.

Note: Table 3-2 is intended as a starting point and is provided by request of field sites and reviewers to facilitate firewall configuration. Use additional references from Apriva, Trust Digital, Microsoft, and DISA STIGs to tailor the firewall rule configuration to the site's specific architecture.

Service	Protocol	Default Port	Comments
Outgoing WTLS connection to the Apriva PMPG or DISA MCEP.	TCP/UDP	12007	Both the Local Gateway Firewall and the Enclave Perimeter firewall outbound rules must be configured to allow this port outbound to Internet via Non-classified Internet Protocol Router Network (NIPRNet) (DoD network). This port is not allowed to traverse the Intranet boundary on the Local Gateway Firewall. (Must traverse PPS CAL boundaries 12, 10, 6, 4, and 2 when configured in compliance with the requirements of this checklist.)
Outgoing connections to all LDAPS servers.	LDAPS	636	To obtain PKI certificate information and revocation lists.
Outgoing connection to trusted OCSP.	HyperText Transfer Protocol (HTTP)	80	To obtain PKI certificate information and revocation lists.
Inbound from handheld user's desktop Web browser or PDA/smartphone Web browser to the Trust Digital Self Service Portal on the TD server	TCP	443	SSL connection
When an ISA Server is used in the Sensa architecture, the Enclave Firewall must be configured to route all Sensa traffic to ISA Server.			Suggestion: Specify all inbound Sensa system IP addresses or all 443 traffic.

Table 3-2. Firewall Architecture Ports, Protocols, and Services

APPENDIX A. REFERENCES

Sensa Server Installation Guide, Release v1.9.2, May 20, 2007.

Sensa System Administration Guide, Release v1.9.2, May 20, 2007.

Trust Digital Version 7.3, Getting Started Guide, Edition 7.3.0, 1 August 2007.

Trust Digital Version 7.3, Administrator's Guide, Edition 7.3.0, 1 August 2007.

This page is intentionally blank.

APPENDIX B. SECURITY POLICY RULES

B.1 SENSa SECURITY POLICY SETTINGS

Policy Rule	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
	Required	Optional				
Delete Signed Unread		Check box	Factory default setting			
Allow Attachments		Check Box	Factory default setting. Set Maximum Message Size. Default is 1000 KiloBytes (KBs)			
Allow Transmission of key Encipherment Certificates		Check Box	Factory default setting			
Preserve Original Signer Certificate		Uncheck box				
Remember CAC PINs While CAC Inserted		Uncheck Box				
Require CAC Inserted for All Sensa Operations		Uncheck Box	Factory default setting			
Time To Live	15 or less			II	WIR1120	
Handheld Signing Notice Rule		Never	Insert optional text, if desired.			
Notice Text			Type in Notice Text if required by local policy			

Table B-1. Sensa Security Policy Rules

B.2 TRUST DIGITAL SECURITY POLICY SETTINGS

Policy Rule	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
	Required	Optional				
System Management/Policy						
Removable Media Encryption Key			This setting is not currently available. TD encryption is disabled with the Sensa system.			
System Management/Compliance Details						
Enable Compliance Enforcement			This setting is not currently available.			
Policy Manager/General Settings						
Enable Encryption			This setting is not currently available. TD encryption is disabled with the Sensa system.			
Encryption Method			This setting is not currently available. TD encryption is disabled with the Sensa system.			
Enable NAM		Do Not Select				
Enable scheduled Check-in		Select				
Scheduled Check-in Interval (min)		30				
Enable Image Management	Enable (check box)			I	WIR1180	
Use Agreement	Enable (check box)			III	WIR0012	
Show Agreement At Device Log-In	Enable (check box)		Enter “I've read & consent to terms in IS user agreement.”	III	WIR0012	

Policy Rule	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
	Required	Optional				
Policy Manager/Password Settings						
Password Type		PIN				
Admin Password	See comments		See Paragraph 3.4 of the checklist for password complexity requirements.	II	WIR1100	
Login Monitor		Enable (check box)	Recommended setting: 30 days			
Enable Password History		Disable (do not check box)				
Number of Passwords Stored		Disable (do not check box)				
Policy Manager/Power On Password						
Minimum Password Length		1	Sensa provides primary device unlock security			
Password delay/Inactivity Timer		Disable (do not check)				
Password Expiration		Disable (do not check)				
Default Password		1				
Password Failure Action		Enable (check box) Enter 5 or less for value. Select “Soft Reset”				

Policy Rule	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
	Required	Optional				
Policy Manager/Firewall Settings						
Enable Firewall	Enable (check box)		Use either default firewall rules or add site specific firewall rule.	II	WIR1250	
Policy Manager/Resource Settings						
Restrict Beam/IR		Enable (check box)				
Restrict Camera		Enable (check box)				
Restrict GPRS		Disable (do not check box)				
Restrict ActiveSync/HotSync		Enable (check box)	Follow Site Security Policy. This is the Universal Serial Bus (USB) connection (ActiveSync) to the desktop.			
Restrict Microphone		Disable (do not check box)				
Restrict SD Card			Follow Site Security Policy			
Restrict Serial USB		Disable (do not check box)				
Restrict Sound			Follow Site Security Policy			

Policy Rule	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
	Required	Optional				
Restrict Wireless	Enable (check box)		Can be enabled only if WLAN requirements of the Wireless STIG are met. See the Wireless Checklist for details.	II	WIR1250	
Restrict SMS		Enable (check box)	If set to Disable (do not check box), IA awareness training must include SMS/MMS security issues.	II	WIR1250	
Restrict All Bluetooth	Enable (check box)			II	WIR1140	
Allow Hands Free	Disable (do not check box)			II	WIR1140	
Allow Serial Port	Enable (check box)			II	WIR1140	

Table B-2. Trust Digital Security Policy Rule

B.3 SYMANTEC ANTIVIRUS FOR HANDHELD CONFIGURATION SETTINGS

Policy Rule	Setting		Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
	Required	Optional				
Auto-Protect	Checked			II	1250	
Last Scan	User will manual scan once per week			II	1250	
Virus Definitions	User will run live update at least once every 2 weeks			II	1250	

Table B-3. Symantec Antivirus Configuration Setting

B.4 HANDHELD SOFTWARE CONFIGURATION SETTINGS

Rule	Setting Required	Optional	Comments	Security Category Code (CAT)	Related Check Number	Check If Open Finding
Sensa Mail>Menu>Options>General Tab						
Default Message Security		Clear Text				
Confirm Delete		Check box				
Allow Read Confirmation		Check box				
Max LDAP Results		20				
Add Signature To Outgoing Messages		Check box				
Auto Signature	If used, must meet requirements listed in Comments		The signature message must not disclose that the email originated from a mobile device (e.g., "Sent From My Windows Mobile Wireless Handheld").	III	WIR1210	

Table B-4. Windows Mobile 5.0 with Sensa & Trust Digital Configuration Settings

This page is intentionally blank.

APPENDIX C. ALLOCATION OF SECURITY REQUIREMENTS TO APRIVA SENSa SYSTEM COMPONENTS

Requirement Number	Requirement	Apriva Sensa V1.9.2	Trust Digital V7.3	Symantec Antivirus V3.5
<p>This table is based on version 2.1, 12 July 2007 of the DoD Wireless Push Email Security Requirements Matrix.</p> <p>Key:</p> <ul style="list-style-type: none"> ✓ Feature implemented by this component in the system. ■ Not Applicable or feature not implemented in the system X Component does not have this capability + Component has this feature but it is not used in the system 				
General Requirements				
1.0	Email redirection from the Exchange Server to the wireless handheld device shall be controlled via centrally managed server. Desktop or Internet controlled email redirection is not authorized.	✓	X	X
2.0	Data Protection Device data will be protected using the following methods to protect DoD data on the handheld when it is lost or stolen. Either Requirement 2.1 or 2.2 must be implemented. Also, Requirement 2.5 must be implemented.	✓	✓	X
2.1	Data Wipe (hard reset) requirements			
2.1.1	The system shall have the capability to perform a "Data Wipe" function whereby all data (operating system, applications, and data) stored in user addressable memory on the handheld device will be erased.	X	✓	X
2.1.2	The system "Data Wipe" function will sanitize all addressable memory locations on the handheld device according to the procedures in the NSA/CSS Policy Manual 9-12 (FOUO). (Note: This is a highly desired capability, not a requirement. The goal is to sanitize the device after a Classified Message Incident (CMI).)	X	X	X
2.2	Data Obfuscation			
2.2.1	The system shall encrypt all data (operating system, applications, and data) stored in user addressable memory on the handheld device using a FIPS certified AES-256 encryption algorithm and a FIPS 140-2 certified encryption module.	✓	+	X
2.2.2	When the Data Obfuscation procedure is implemented, the AES encryption key shall be deleted, scrambled, or hidden such that it is no longer available to decrypt the device data.	✓	X	X
2.3	A highly desirable, but not required, feature is the capability to "Data Protect" all removable storage media.	X	+	X

Requirement Number	Requirement	Apriva Sensa V1.9.2	Trust Digital V7.3	Symantec Antivirus V3.5
2.4	Remote Data Protection The system shall provide remote data protection capabilities using one or both of the following methods (2.4.1 or 2.4.2):	✓	✓	X
2.4.1	The system administrator shall have the capability transmit a remote Data Protection (e.g., "Data Wipe" or "Data Obfuscation") command to the handheld device.	✓	✓	X
2.4.2	The system will automatically perform a "Data Protection" procedure ("Data Wipe" or "Data Obfuscation") after a set period of time the device has not contacted the management server.	X	X	X
2.4.2.1	The required "server no-contact" period shall be configurable from 1 day to 14 days.	X	X	X
2.5	The system shall enforce user authentication to unlock the device and automatically perform a "Data Protection" procedure after a set number of incorrect authentication attempts occur. See Requirements 21.0 and 30.4 for additional information.	✓	+	X
3.0	Encryption of transmitted data/email			
3.1	All data (including email attachments) sent over the wireless link from the PDA/smartphone to the wireless email server located on the DoD network will be encrypted using FIPS 140-2 validated cryptographic modules. The available encryption algorithms will be restricted to 3DES and/or AES. (Note: Support for AES only may be required by some DoD sites.)	✓	X	X
3.2	All updates / rekeying of the link encryption key used to encrypt email on the wireless link shall be controlled by the wireless email server located on the DoD network	✓	X	X
3.3	AES shall be available as the master or session key algorithm.	✓	X	X
3.4	The rekey period will be 30 days or less.	✓	X	X
4.0	S/MIME requirements			
4.1	The system will be capable of providing S/MIME v3 (or later version) encryption of email. FIPS 140-2 validated cryptographic modules will be used by the S/MIME service for data in transit.	✓	X	X
4.2	S/MIME shall be fully interoperable with DoD PKI and CAC. CAC (hard token) and PKCS#12 (soft token) certificate stores should be supported.	✓	X	X
4.2.1	The S/MIME encryption key shall be 3DES or AES (128-bit minimum key length)	✓	X	X

Requirement Number	Requirement	Apriva Sensa V1.9.2	Trust Digital V7.3	Symantec Antivirus V3.5
4.2.2	Path Processing: system must verify all digital certificates in the path (user certs, intermediate certs, and root certs)	✓	X	X
4.2.2.1	It is required that DoD root and intermediate certs be stored on the handheld device	✓	X	X
4.2.3	A user should have the ability to save public certs of contacts in the contact object by one or both of the following methods: 1. by saving public certs to the contacts object that were attached to a received email message 2. by saving public certs to the contacts object downloaded via a GDS LDAP lookup from the handheld device	✓	X	X
4.2.4	A user should be able to check the status of the cert on a received or outgoing message without having to be connected to the email management server (desired, but optional requirement).	✓	X	X
4.2.4.1	It is recommended (but not required) that the certificate status be cached on the handheld device for a period of not more than 7 days.	X	X	X
4.2.5	If SCR PIN caching is available, the system administrator shall be able to set the timeout period. Timeout period should be able to be set from 15 to 120 minutes).	X	X	X
5.0	If the wireless email system provides text messaging services (e.g., PIN-to-PIN messaging), the service will be S/MIME enabled.	X	X	X
5.1	Information sent via available text messaging services should be logged. This is an optional, but recommended capability.	X	X	X
6.0	If the wireless email service provides wireless activation / provisioning of the handheld device, the following requirements must be met:			
6.1	The system administrator shall have the capability to disable OTA provisioning.	X	✓	X
6.2	A trusted loading process must be the foundation for device provisioning (whether tethered or over-the-air).	X	✓	X
6.2.1	The trusted OTA provisioning process must provide mutual authentication between the provisioning server and the provisioned device.	X	✓	X
6.2.2	The trusted OTA provisioning process must provide data integrity and confidentiality of the provisioning data downloaded from the server to the handheld device.	X	✓	X

Requirement Number	Requirement	Apriva Sensa V1.9.2	Trust Digital V7.3	Symantec Antivirus V3.5
7.0	Internet connections.			
7.1	The system administrator shall have the capability to remove the wireless carrier's Internet browser icon from the handheld device screen during provisioning of the handheld device or configure the system to satisfy requirement 7.2.	X	✓	X
7.2	The system administrator shall have the capability to configure the browser to connect only to a specific URL (e.g., DoD network VPN gateway, DoD web proxy) during provisioning of the handheld device. The user shall not be able to override this setting.	X	✓ SSL authentication issue	X
7.3	The desire is to require users to browse the Internet through a secure encrypted tunnel (using a FIPS 140-2 validated cryptographic module) to the DoD network Internet gateway.	X	X	X
7.4	System shall provide the capability for the handheld device browser to support CAC authentication to web sites that require CAC authentication of users. (See Requirement 9.1)	X	X	X
8.0	The system shall have the capability to log all security events (e.g., user logon, logoff, system admin configuration changes).	Some	X	X
8.1	The system shall have the capability to send email alert notifications to the system administrator when specific system log events occur. Optional requirement.	X	X	X
8.2	The system should have the capability to audit certain Bluetooth-related device-level events that identify changes to security settings, incoming or outgoing connection requests (including Bluetooth device addresses), failed authentication attempts, and other unauthorized activity. This is an optional, but recommended capability.	X	X	X
9.0	A user shall be required to enter user authentication credentials using Smart Card Login (SCL) prior to gaining access to any DoD network services (e.g., internal network web servers) other than push email via the wireless email connection with the DoD network.. (Note: This authentication is separate from user authentication for unlocking the handheld device.)	N/A	N/A	N/A
9.1	User SCL authentication support for access to network and web services shall be fully interoperable with DoD PKI and CAC. (See Requirement 7.4)	X	X	X

Requirement Number	Requirement	Apriva Sensa V1.9.2	Trust Digital V7.3	Symantec Antivirus V3.5
10.0	Mutual authentication shall be used to during the process to establish a connection between the email server and the wireless handheld device (certificate based authentication is desired but not currently required).	✓	X	X
10.1	If certificate based authentication is used between the handheld device and the email server, the handheld device certificate will not be importable to the device or subsequently exportable from the device.	✓	X	X
Policy Management Requirements				
20.0	System must centrally enforce security policies on the handheld device. The following policies shall be available:	✓	✓	X
21.0	The system administrator shall be able to select either PIN or Smart Card Login (SCL) for user authentication to unlock the device.	✓ (Only supports SCL)	+ (Only supports PIN)	X
21.1	If a PIN is used to unlock the device (vice SCL), the PIN policy must meet the following requirements (all configurable by the system administrator and controlled by a centrally managed policy rule):	X	+	X
21.1.1	Maximum password age (e.g., 30 days, 90 days, 180 days)	X	+	X
21.1.2	Minimum password length. The system will allow the sys admin to specify exact required length of the password (a range of 5 to 12 characters is the minimum requirement).	X	+	X
21.1.3	Maximum Password attempts. Device will perform a Data Protection command (see Requirements 2.0 and 30.4) after a set number of incorrect passwords are entered. The system will allow the sys admin to specify exact number of incorrect passwords before the device will perform a Data Protection command (a range of at least 3-10 is the minimum requirement).	X	+	X
21.1.4	Maximum password history. The system will allow the sys admin to specify exact number of previous passwords that cannot be used (1-5 is the minimum requirement).	X	+	X
21.1.5	Several different password compositions (i.e., pattern checks) should be available, to include upper and lower case letters, numbers, and special characters, to allow administrators to tailor the password policies to fit unique organizational requirements.	X	+	X

Requirement Number	Requirement	Apriva Sensa V1.9.2	Trust Digital V7.3	Symantec Antivirus V3.5
21.2	If SCL authentication is used for unlocking the handheld device, the SCL shall be fully interoperable with DoD PKI and CAC.	✓	+	X
22.0	The handheld device has an inactivity timeout whereby the user must reenter their user PIN or Smart Card PIN to unlock the device. Shall be configurable. The following settings shall be available, at a minimum: Disable (no timeout), 15 minutes, & 60 minutes.	✓	+	X
23.0	The system shall control the capability of the user to install or de-install third party applications on the handheld device.	X	✓	X
24.0	Data-at-Rest Protection			
24.1	The system shall have the capability to encrypt all user data at rest stored on the handheld device.	✓	+	X
24.2	FIPS 140-2 validated encryption (AES-256 preferred; 3DES or AES required (Note, some DoD sites may require AES only)) shall be used for data-at-rest protection.	✓	+	X
24.3	A highly desirable feature (but not required) is the capability to encrypt all removable storage media.	X	+	X
25.0	Bluetooth requirements: (Note, currently, Bluetooth is only authorized for handheld device connection to approved Bluetooth enabled Smart Card Readers (SCR). All other Bluetooth services are not authorized.)			
25.1	Bluetooth service and profile requirements			
25.1.1	Except for the Serial Port profile, all Bluetooth services/profiles, user controls, and applications must either be removed from the host device or reliably disabled.	✓	✓	X
25.1.2	The Bluetooth Serial Port can only be used with a Bluetooth SCR	✓	X	X
25.2	The system administrator shall have the capability to disable the following if not already permanently disabled: Note: the Bluetooth features listed below will be enabled by the system/system administrator only when a Bluetooth SCR is used.	✓	X	X
25.2.1	-Bluetooth radio and/or Bluetooth connectable mode.	✓	✓	X
25.2.2	-Discoverable mode	✓	✓	X
25.2.3	-Serial Port profile	✓	✓	X

Requirement Number	Requirement	Apriva Sensa V1.9.2	Trust Digital V7.3	Symantec Antivirus V3.5
25.3	The system shall have the following Bluetooth capabilities:	✓	X	X
25.3.1	Bluetooth pairing using a randomly generated passkey size of at least 8 digits	X (N/A SCR tethered to handheld during pairing)	X	X
25.3.2	Bluetooth mutual authentication immediately after the initial establishment of any Bluetooth connection between the handheld and the SCR	X (N/A SCR tethered to handheld during pairing)	X	X
25.3.3	128 bit Bluetooth encryption	✓	X	X
25.3.4	FIPS 140-2-certified cryptography of data-in-transit over the Bluetooth link. Note: It expected that the data transmission between the SCR and the handheld be encrypted with FIPS 140-2 certified encryption. This encrypted data payload will then be encrypted by the 128-bit encryption provided by the Bluetooth protocol.	✓	X	X
25.3.5	Bluetooth devices should only use Class 2 or 3 standard radios. Class 1 radios are not permitted. Radio modifications (e.g., signal amplification, antenna modification) are not permitted.	✓	X	X
25.3.6	Bluetooth Device Addresses (BD_ADDRs) should not be visibly printed on the outside of the device.	✓	X	X
25.3.7	Random passkeys must be newly generated for each Bluetooth pairing.	X (N/A SCR tethered to handheld during pairing)	✓	X
25.4	For Bluetooth SCR, the system shall have the following capabilities: -Adjustment for the maximum Bluetooth range Note: this is a desired, but not required, feature.	X	X	X
26.0	The system administrator shall have the capability to disable the following wireless services on the handheld device:			
26.1	-Text Messaging (SMS)	X	✓	X
26.2	-MMS	X	✓	X

Requirement Number	Requirement	Apriva Sensa V1.9.2	Trust Digital V7.3	Symantec Antivirus V3.5
27.0	The system administrator shall have the capability to enable or disable the following PKI related configuration settings on the handheld device or alternatively, the system will provide the user the capability to accept or not accept a certificate with the following characteristics: (Note: the desire is to have the certificate policy on the handheld device (e.g., accept/not accept certificates with specific characteristics) mirror the practice used on DoD workstations.)	✓	X	X
27.1	-Revoked certificate use	✓	X	X
27.2	-Unverified certificate use	✓	X	X
27.3	-Untrusted certificate use	✓	X	X
27.4	-Non-FIPS approved algorithm used in certificate	✓	X	X
27.5	-Invalid certificate use	✓	X	X
27.6	-Unverified CRL use	✓	X	X
28.0	Handheld device IR port, radio (WiFi, BT, WiMax, etc.), voice recorder, microphone, camera, memory card port can be disabled by system central IT policy management software. (Note: There is no requirement that the services listed above remain disabled after a hard reset (device wipe) of the PDA.)	X	✓	X
29.0	Compliance verification. The Security system will verify that the handheld device meets compliance requirements prior to allowing a connection to the email system or network resources. (This is highly desired feature, but not required at this time.) Desired compliance checking include the following:	X	+	X
29.1	Security Policy management client installed	X	+	X
29.2	Security Policy enabled	X	+	X
29.3	Antivirus application installed and up-to-date	X	X	X
29.4	Operating System patches up-to-date	X	✓	X
29.5	Firewall application installed and configured according to system security policy	X	✓	X
Handheld Device Requirements				
30.0	User authentication to unlock handheld device			

Requirement Number	Requirement	Apriva Sensa V1.9.2	Trust Digital V7.3	Symantec Antivirus V3.5
30.1	The handheld device must be protected by authenticated logon using a PIN or smart card logon (SCL).	✓ (SCL only)	+	X
30.2	A user cannot bypass handheld device authentication.	✓	+	X
30.3	When CAC authentication is enabled, a user cannot bypass this feature and use password authentication	✓	+	X
30.4	When password authentication is enabled, the handheld device will automatically perform a Data Protection command ("Data Wipe" or "Data Obfuscation") after X number of unsuccessful password authentication attempts are made. The value of X is set by IT policy management control. (See requirements 2.0 and 21.0 for additional information.)	X	+	X
31.0	Digital credential migration			
31.1	The handheld device shall support credential migration in a secure manner by credential owner if device is to be re-provisioned (e.g., system/application software reloaded).	✓	X	X
31.2	The handheld device shall support credential migration in a secure manner by credential owner when user gets a new CAC.	✓	X	X
32.0	Digital signing/encrypting/decrypting messages			
32.1	The user shall have the capability to digitally sign and/or encrypt outgoing email messages using software or hardware based digital certificates.	✓	X	X
32.2	The user shall have the capability to decrypt incoming email messages using software or hardware based digital certificates	✓	X	X
32.3	The system shall provide a mechanism to provide certificate validation through either trusted OCSP, CRLs, or SCVP.	✓	X	X
32.3.1	The system shall provide a noticeable warning to the user if the CRL, SCVP, or OCSP server cannot be contacted (highly desired, but optional).	✓	X	X
32.4	The system shall support LDAP/LDAPs (as soon as practical after protocol approval). (This is the mechanism that allows the user to do ad-hoc public certificate lookups and retrievals using LDAP.)	✓	X	X
33.0	DoD approved antivirus software shall be operated on the handheld device.	X	X	✓

Requirement Number	Requirement	Apriva Sensa V1.9.2	Trust Digital V7.3	Symantec Antivirus V3.5
34.0	DoD approved personal firewall software shall be operated on the handheld device. The firewall shall be able to filter both inbound and outbound traffic based on ports, protocols, and IP address.	X	✓	X

Table C-1. Allocation of DoD Security Requirements to System Components

APPENDIX D. CAC DIGITAL CERTIFICATE PROVISIONING

1. Initial Provisioning of Windows Mobile 5.0 Handhelds with Sensa for S/MIME

The user's public certs are loaded on the Windows Mobile device during the initial provisioning process. Refer to paragraph 3.3.2 for detailed instructions.

2. Loading New CAC Public Certificates on a Windows Mobile Handheld

When a Sensa user gets a new CAC after the initial provisioning of the Windows Mobile device, the following procedures should be followed for loading the new CAC public certificates on the Windows Mobile device:

- Backup data files on the Windows Mobile device.
- Perform a Hard Reset of the device.
- Perform steps in paragraph 3.3.2 to reload all software on the device (initial provisioning).

3. Sending Encrypted Email

Prior to sending an encrypted e-mail, the Sensa user should set up a contact in their address book on the handheld and save the recipients public digital certificates to the recipients contact object. There are several methods that can be used for obtaining a contact's digital certificates:

- The user can query an admin-configured LDAP server (DISA or JITC for example) for the public cert and save it on the device against the contact object
- The user can query the GAL for the public cert and save it on the device against the contact object
- The user can save the cert from a signed message on the device against the contact object
- The user can sync his/her Outlook Contacts that have the certificates associated with the objects to the device.

For additional information or assistance on Apriva Sensa PKI issues, contact the DoD Public Key Encryption (PKE) office at pke_support@disa.mil or visit their Web site at <https://gesportal.dod.mil/sites/dodpke/>.

This page is intentionally blank.

APPENDIX E. VMS PROCEDURES

The following information applies only to teams and sites that use VMS to enter and track DoD assets. When conducting an Apriva Sensa Security Readiness Review (SRR), the Team Lead and the assigned Reviewer identify security deficiencies, provide data from which to predict the effectiveness of proposed or implemented security measures associated with the Sensa system and operating environment. SRR of a DoD Sensa system requires that the results of the SRR be tracked using the VMS database.

Both the Reviewer and the SA will create, maintain, and track assets in VMS. The Reviewer will use the Asset and Finding Maintenance screen to perform these functions. The SA will use the By Location navigation chain to perform the same function. When Reviewers access the Asset and Finding Maintenance screen, the Navigation pane displays a white Visits folder. Expand this Visits folder to display its subfolders. Each subfolder represents an individual visit in VMS that is assigned for review. Click (+) to expand the visit and display the location summaries for the visit. Within the location, Windows Mobile assets are tracked using the Computing asset type.

Use the following matrix to select the appropriate asset type for each Windows Mobile Sensa asset. The Reviewer or SA must enter the entire asset posture including non-wireless related applications and services installed on the Sensa servers.

VMS Asset Matrix		
Computing – Assets with an OS such as a wireless email server or wireless email handheld device.		
Non-Computing – Used for registering wireless networks. Applies general wireless networking environment policies.		
Wireless Technology	VMS Asset Type	ASSET POSTURE
All wireless devices (Wireless e-mail servers and handheld devices)	Non-Computing	Network Policy Requirements -> Wireless Policy Note: These checks apply to the network or concern site policy rather than to a specific wireless device.
Apriva Sensa Server Note: Only configure asset for applications installed on the same server as the Apriva Sensa Server.	Computing	Operating System -> Windows. Expand and select version then service pack installed. Application>Wireless Email Server – Apriva Sensa Server Application ->Antivirus. Expand and select version. Application – Expand and select other applications installed on same server to capture the entire asset posture of the server (e.g., SQL, Exchange, Browsers, Office Automation, etc). Role – Member Server

VMS Asset Matrix		
Computing – Assets with an OS such as a wireless email server or wireless email handheld device. Non-Computing – Used for registering wireless networks. Applies general wireless networking environment policies.		
Wireless Technology	VMS Asset Type	ASSET POSTURE
Trust Digital Security Server(s) Note: Only configure asset for applications installed on the same server as the Trust Digital Security Server(s) application.	Computing	Operating System -> Windows . Expand and select version then service pack installed. Application>Wireless Email Server – Trust Digital Security Server Application ->Antivirus. Expand and select version. Application – Expand and select other applications installed on same server to capture the entire asset posture of the server (e.g., SQL, Exchange, Browsers, Office Automation, etc). Role – Member Server
Windows Mobile Sensa Client Devices	Computing	Note: Do not mark as a workstation Note: Do not enter IP or Media Access Control (MAC) address Network -> Data Network -> Wireless -> Wireless Email -> Apriva Sensa Client
Wireless Policy	Non-Computing	Network Policy Requirements -> Wireless Policy

Table E-1. VMS Asset Matrix

This page is intentionally blank.